



## **Mandanteninfo 05/2015: Die europäische Datenschutzrichtlinie ([RiLi 95/46/EG](#)) verbietet die Möglichkeit personenbe- zogene Daten auf amerikanischen Servern zu speichern**

### **EuGH: Safe-Harbor-Entscheidung der EU-Kommission ist ungültig**

*EuGH, [Urteil vom 06.10.2015 – C – 362/14](#), Maximilian Schrems gegen Data Protection Commissioner*

**1. [Artikel 25 Abs. 6 der Richtlinie 95/46/EG](#) vom 24.10.1995 ist im Lichte des Artikel [7](#), [8](#) und [47](#) der Charta der Grundrechte der EU dahingehend auszulegen, dass eine aufgrund dieser Bestimmung ergangene Entscheidung über die Angemessenheit des durch „Safe-Harbor“ gewährleisteten Schutzes, in der die EU-Kommission festgestellt hat, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine nationale Datenschutzbehörde nicht daran hindert, die Beschwerde einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten, die aus einem EU-Land übermittelt werden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis des Drittlandes keinen angemessenen Schutz gewährleistet.**

**2. Die Entscheidung [2000/520](#) (Safe-Harbor-Entscheidung) ist ungültig.**

#### **1. Der Fall:**

Bereits im Jahr 2010 hat die Konferenz der deutschen Datenschutzbeauftragten am 18. und 19.03.2010 in Wiesbaden ausgeführt, dass die Erklärung über eine Selbstzertifizierung, wie sie die Safe-Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht um dem deutschen Datenschutzrecht und der europäischen Datenschutzrichtlinie Rechnung zu tragen. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe-Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in den USA übermittelte personenbezogene Daten zugreifen und damit die Safe-Harbor-Grundsätze gravierend verletzen, da im Rahmen des US Patriot Act, US-Sicherheitsbehörden auch ohne Benachrichtigung der Dateninhaber Zugriff auf die in US-Clouds gespeicherten Daten gewährt werden muss. Nach diesen Enthüllungen hatte der österreichische Staatsbürger Maximilian Schrems, als Nutzer des sozialen Netzwerks Facebook, Beschwerde bei der irischen Datenschutzbehörde (Commissioner) eingelegt, da alle im Unionsgebiet der EU wohnenden Personen, die Facebook nutzen wollen, bei ihrer Anmeldung einen Vertrag mit Facebook Irland, einer Tochtergesellschaft der in den Vereinigten Staaten ansässigen Facebook Inc. abschließen müssen. Die personenbezogenen Daten der in der EU wohnenden Nutzer von Facebook werden ganz oder teilweise an den Server der Facebook Inc., die sich in den Vereinigten Staaten befinden, übermittelt und dort verarbeitet. Im Juni 2013 legte Herr Schrems bei der irischen Datenschutzbehörde eine Beschwerde ein, mit der er die Behörde im Wesentlichen aufforderte in Ausübung der der Behörde übertragenen Befugnisse Facebook Irland zu untersagen, seine personenbezogenen Daten in die Vereinigten Staaten zu übermitteln. Er machte geltend, dass das Recht und die Praxis der Vereinigten Staaten keinen ausreichenden Schutz der personenbezogenen Daten vor der Überwachungstätigkeit der US-Sicherheitsbehörden gewährleisten. Dabei verwies er auf die von Edward Snowden enthüllten Tätigkeiten der NSA. Die irische Datenschutzbehörde wies die Beschwerde von Herrn Schrems als unbegründet zurück mit der Begründung, dass es keinen Beweis für den Zugriff der NSA auf die personenbezogenen Daten von Herrn Schrems gäbe. Daraufhin erhob Herr Schrems Klage vor dem irischen „High Court“. Der irische „High Court“ stellte fest, dass die elektronische Überwachung und Erfassung der aus der EU in die Vereinigten Staaten übermittelten personenbezogenen Daten unerlässlichen Zielen von öffentlichem Interesse diene. Die Enthüllungen von Herrn Snowden hätten jedoch gezeigt, dass die NSA und andere US-amerikanische Bundesbehörden „erhebliche Exzesse“ begangen hätten. Unter diesen Umständen hat der „High Court“ beschlossen, das Verfahren auszusetzen und dem Europäischen Gerichtshof zur Vorabentscheidung vorzulegen.

### **Die Entscheidung:**

Aufgrund der verschiedenen Vorlagefragen, die der irische „High Court“ stellte, kam der Europäische Gerichtshof zu dem Ergebnis, dass die [Richtlinie 95/46 EG](#), soweit sie die Verarbeitung personenbezogener Daten regelt, die zu Beeinträchtigungen der Grundfreiheiten und des Rechts auf Achtung der Privatsphäre führen kann, notwendigerweise im Lichte der durch die Charta garantierten Grundrechte auszulegen ist. Damit gewährleiste die [Richtlinie 95/46 EG](#) nicht nur einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechten natürlicher Personen, insbesondere des Grundrechts auf Achtung der Privatsphäre, bei der Verarbeitung personenbezogener Daten, sondern auch ein hohes Schutzniveau dieser Grundrechte und Grundfreiheiten. Weiter stellt der Europäische Gerichtshof fest, dass die nationalen Datenschutzbehörden hinsichtlich der Übermittlung personenbezogener Daten in Drittländer die Aufgabe habe in völliger Unabhängigkeit die Einhaltung der Unionsvorschriften über den Schutz natürlicher Personen bei Verarbeitung solcher Daten zu überwachen. Die Gewährleistung der nationalen Datenschutzbehörden soll die wirksame und zuverlässige Kontrolle der Einhaltung der entsprechenden Vorschriften sicherstellen. Die Schutzfunktion solcher nationalen unabhängigen Kontrollbehörden stellt damit ein wesentliches Element zur Wahrung des Schutzes der Person bei Verarbeitung personenbezogener Daten dar. Um einen wirksamen Schutz der Grundrechte und Grundfreiheiten zu gewährleisten, hätten die Datenschutzbehörden zur Erfüllung ihrer Aufgaben umfassende Informations- und Eingriffsbefugnisse. Diese beziehen sich zwar zunächst nur auf das Hoheitsgebiet ihres Mitgliedsstaates, so dass [Artikel 28 der Richtlinie 95/46 EG](#) ihnen keine Befugnis in Bezug auf die Verarbeitung solcher Daten im Hoheitsgebiet eines Drittlandes verleiht. Die Übermittlung personenbezogener Daten aus einem Mitgliedsstaat in ein Drittland stellt jedoch als solche eine Verarbeitung personenbezogener Daten dar, die im Hoheitsgebiet eines Mitgliedsstaates vorgenommen wird. In der [Richtlinie 95/46 EG](#) selbst ist jedoch geregelt, dass die Übermittlung personenbezogener Daten in Drittländer nur unter voller Einhaltung der Rechtsvorschriften erfolgen dürfen, die die Mitgliedsstaaten gemäß dieser Richtlinie erlassen haben. Eine solche Datenübermittlung ist jedoch nur zulässig, wenn die Drittländer selbst ein angemessenes Schutzniveau gewährleisten.

Nach alledem ist eine nationale Datenschutzbehörde nicht daran gehindert festzustellen, ob ein Drittland ein angemessenes Schutzniveau gewährleistet.

2. Zur Gültigkeit der Safe-Harbor-Grundsätze führt der Gerichtshof im weiteren aus, dass das Wort „angemessenes Schutzniveau“ in [Artikel 25 Abs. 6 der Richtlinie 95/46 EG](#) nicht verlangt, dass in einem Drittland ein dem in der Unionsordnung garantiertes identisches Schutzniveau gewährleistet, dass jedoch zum Schutze der Grundfreiheiten und Grundrechte im Lichte der Grundrechtecharta ein gleichwertiges Schutzniveau garantiert werden müsse. Ohne ein solches Erfordernis würde nämlich das in der Richtlinie erwähnte Ziel missachtet. Außerdem könnte das durch die [Richtlinie 95/46 EG](#) im Lichte der Grundrechtecharta garantierte hohe Schutzniveau leicht umgangen werden, indem personenbezogene Daten aus der Union heraus in Drittländer übermittelt werden, um dort verarbeitet zu werden.

Die Safe-Harbor-Grundsätze lassen den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen der USA den Vorrang vor den Grundsätzen des Safe-Harbor. Aufgrund dieses Umstandes sind die selbstzertifizierten US-Unternehmen oder sonstiger Organisationen, die personenbezogene Daten aus einem EU-Land erhalten, ohne jede Einschränkung verpflichtet, die Grundsätze des Safe-Harbor unangewendet zu lassen, wenn sie im Widerstreit zu den genannten Erfordernissen in den USA stehen. Überdies enthalten die Safe-Harbor-Grundsätze keinerlei Regelung dazu, Grundrechtseingriffe in den USA zu begrenzen. Es fehle ein wirksamer gerichtlicher Rechtsschutz gegen derartige Eingriffe, weshalb ein angemessenes Schutzniveau in den USA nicht gewährleistet sei. Aus diesem Grunde sei ohne dass es einer Prüfung des Inhalts der Grundsätze des Safe-Harbor im Übrigen bedarf, der Schluss zu ziehen, dass die Safe-Harbor-Erklärung gegen die Vorschrift des [Artikel 25 Abs. 6 der Richtlinie 95/46 EG](#) verstößt und aus diesem Grunde ungültig ist.

### **Anmerkung:**

Die Entscheidung ist vollumfänglich zu begrüßen und eröffnet den Betriebsräten zahlreiche Handlungsmöglichkeiten über den Datenschutz von personenbezogenen Daten im Unternehmen und Konzern nochmals zu diskutieren, dies gilt vorliegend jedoch nicht nur für Unternehmen die ihre Daten nach Safe-Harbor in Drittstaaten übermitteln, sondern auch für solche Unternehmen, die dies auf konzerninterner Grundlage, d. h. auf Basis sog. Binding Corporate Rules tun. Ein erster Schritt sollte sein, sich bei den Unternehmensleitungen schlau zu machen, welche Daten in den USA, Indien, China oder einem sonstigen Drittland verarbeitet werden und wie gewährleistet werden kann, dass die Grundrechte und Rechte auf informationelle Selbstbestimmung eingehalten werden.

### **[Sie interessieren sich für andere Ausgaben?](#)**

<http://www.arbeitsrecht24.com/mandanteninfo.php>

